Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

POSTULATE-SETS FOR ABELIAN GROUPS AND FIELDS.

By Wallie Abraham Hurwitz.

Postulate-sets for fields have been given by Dickson* and Huntington;† these have naturally been founded on previous definitions of abelian groups. Several years ago the writer gave a postulate-set for abelian groups‡ which not only (like a set of Huntington's on which it was based) made no assumption of closure with respect to the group operation, but also replaced both the associative and commutative laws by a single law of somewhat the same character as the associative law. The present paper contains a slightly altered form of this definition and an extension to the case of fields. The postulate-set for fields contains five postulates, aside from one specifying the cardinal number of the class,—thus reducing by two postulates (one each for addition and multiplication) the smallest number used hitherto. As an incidental result a new type of finite linear algebras is found, obeying the commutative law and admitting unique division by non-zero elements, but not obeying the associative law or containing an idemfacient element.§ It need scarcely be mentioned that a definition of groups or fields which introduces closure, associativity, and commutativity as theorems rather than as postulates is justified by its logical interest, and not by any practical use.

The proofs in the paper are complete in themselves and may be read independently of previous postulate-sets for groups and fields.

1. Definition of Abelian Groups. A class K with an operation $\circ$ between pairs of elements will be called an abelian group if the following postulates hold:

(1) *If* a, b, c, $a \circ b$, $c \circ b$, *and* $a \circ (c \circ b)$ *belong to* K, *then* $(a \circ b) \circ c = a \circ (c \circ b)$.

(2) *If* a *and* b *belong to* K, *there is an element* x *of* K *such that* $a \circ x = b$.

The number of elements is specified by adding one of the postulates:

(N_n) *K contains n elements.*

(N') *K is countably infinite.*

(N'') *K has the cardinal number of the continuum.*

---

* Transactions of the American Mathematical Soc ety, vol. 4 (1903), p. 13; vol. 6 (1905), p. 108; Göttinger Nachrichten (1905), p. 358.

† Transactions of the American Mathematical Society, vol. 4 (1903), p. 31; vol. 6 (1905), p. 181.

‡ These *Annals*, Second Series, vol. 8 (1907), p. 94.

§ I. e., an element whose product with any element reproduces the latter.

Every abelian group satisfies (1) and (2), and abelian groups exist satisfying each of (N_n) (for any positive integer n), (N'), (N''). It will be shown that conversely the ordinary properties of an abelian group follow from (1), (2).

In the first place, if a, b, and either $a \circ b$ or $b \circ a$ belong to K, then

$$a \circ b = b \circ a.$$

Suppose, for example, that $a \circ b$ belongs to K. By (2) take x so that $a \circ x = b$; then by (1),

$$a \circ (a \circ x) = (a \circ x) \circ a, \quad \text{or} \quad a \circ b = b \circ a.$$

We now show, with the aid of this result, that for any two elements a, b of K, $a \circ b$ is an element of K. By (2) take successively x, y, z, w, so that

$$b \circ x = a, \quad a \circ y = x, \quad y \circ z = a, \quad a \circ w = z.$$

Then by (1),

$$a = y \circ z = y \circ (a \circ w) = y \circ (w \circ a) = (y \circ a) \circ w = x \circ w,$$

so that

$$b \circ x = a = x \circ w = w \circ x,$$

and

$$z = a \circ w = w \circ a = w \circ (b \circ x) = (w \circ x) \circ b = a \circ b;$$

therefore $a \circ b$ is the element z known to belong to K.

Since $a \circ b$ belongs to K and the commutative law holds, we see from (1) that the associative law holds; these results, with (2), comprise one of the ordinary forms of definition of abelian groups.

The postulates (1), (2), with any of (N_n) $(n > 1)$,[*] (N'), (N'') are independent. The proof will appear as part of the corresponding work for fields.

2. Definition of Fields. A class K, with two operations $\oplus$ and $\otimes$ between pairs of elements, will be called a field if the following postulates hold:

$(A1)$ *If* a, b, c, $a \oplus b$, $c \oplus b$, *and* $a \oplus (c \oplus b)$ *belong to* K, *then*

$$(a \oplus b) \oplus c = a \oplus (c \oplus b).$$

$(A2)$ *If* a *and* b *belong to* K, *there is an element* x *of* K *such that*

$$a \oplus x = b.$$

$(M1)$ *If* a, b, c, $a \otimes b$, $c \otimes b$, *and* $a \otimes (c \otimes b)$ *belong to* K, *then*

$$(a \otimes b) \otimes c = a \otimes (c \otimes b).$$

---

[*] If $n = 1$, postulate (2) is sufficient.

($M2$) *If* a *and* b *belong to* K *and* $a \oplus a \neq a$, *there is an element* x *of* K *such that*

$$a \otimes x = b.$$

(D) *If* a, b, c, $a \otimes b$, $a \otimes c$, $b \oplus c$, *and* $(a \otimes b) \oplus (a \otimes c)$ *belong to* K, *then*

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c).$$

We specify the number of elements by adding one of the postulates (N_n) ($n > 1$), (N'), (N'') of the preceding section.

Postponing inquiry as to whether (or when) the postulates are consistent and independent, we proceed to show that the concept defined by ($A1$), ($A2$), ($M1$), ($M2$), (D) agrees with the usual notion of a field. Any field in the ordinary sense satisfies ($A1$), ($A2$), ($M1$), ($M2$), (D); we have then to show that conversely these postulates imply the field properties.

Since ($A1$), ($A2$) are precisely (1), (2) with $\oplus$ for $\circ$, we have at once:

THEOREM I. *K is an abelian group with respect to* $\oplus$.

Among the consequences of this theorem we note particularly: when a and b belong to K, then $a \oplus b$ belongs to K; one and only one element of K (the "identity" of the group, which we may call 0) satisfies the condition

$$a \oplus a = a;$$

from

$$a \oplus x = a$$

follows $x = 0$ and conversely.

LEMMA. *If* a *and* $a \otimes 0$ *belong to* K, *then* $a \otimes 0 = 0$.

In case $a = 0$, we have by (D)

$$0 \otimes (0 \oplus 0) = (0 \otimes 0) \oplus (0 \otimes 0)$$

or

$$(0 \otimes 0) \oplus (0 \otimes 0) = 0 \otimes 0,$$

whence

$$0 \otimes 0 = 0.$$

Suppose then $a \neq 0$. By ($A2$) choose x so that

$$(a \otimes 0) \oplus x = 0,$$

and by ($M2$) choose y so that

$$a \otimes y = x.$$

Then by (D),

$$a \otimes (0 \oplus y) = (a \otimes 0) \oplus (a \otimes y)$$

or

$$x = (a \otimes 0) \oplus x,$$

and therefore

$$a \otimes 0 = 0.$$

If we now denote by K' the class obtained by removing from K the element 0, we have:

THEOREM II. *K' is an abelian group with respect to* $\otimes$.

Since any element of K' is an element of K, ($M1$) implies (1) with $\otimes$ for $\circ$ and K' for K. Also the hypothesis of ($M2$) implies the hypothesis of (2); in order to see that the conclusion of (2) agrees with the conclusion of ($M2$) we need only ascertain that the x defined is in K', i. e., that $x \neq 0$. This is assured by the preceding lemma; for the hypothesis $a \otimes x = b$, $x = 0$ would imply $b = 0$, so that b would not be in K'. As a consequence we note: if a and b belong to K', then $a \otimes b$ belongs to K'; or, in other words, if a and b belong to K and $a \neq 0$, $b \neq 0$, then $a \otimes b$ belongs to K and $a \otimes b \neq 0$.

THEOREM III. *If a belongs to K, then* $a \otimes 0 = 0 \otimes a = 0$.

First suppose $a \neq 0$. By ($M2$) take x so that

$$a \otimes x = 0;$$

theorem II shows that the assumption $x \neq 0$ would involve

$$a \otimes x \neq 0,$$

which is untrue; hence $x = 0$ and $a \otimes 0 = 0$. By ($M1$),

$$(a \otimes 0) \otimes a = a \otimes (a \otimes 0);$$

hence

$$0 \otimes a = a \otimes 0 = 0.$$

Consider now the case $a = 0$. Choose $x \neq 0$. By ($A2$) take y so that

$$x \oplus y = 0;$$

evidently $y \neq 0$. Then by (D),

$$0 \otimes (x \oplus y) = (0 \otimes x) \oplus (0 \otimes y),$$

or by the part of the theorem already proved, $0 \otimes 0 = 0 \oplus 0 = 0$.

We now restate (D) in modified form as:

THEOREM IV. *If a, b, c belong to K, then* $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$.

Theorems I–IV exhibit the properties of a field in the ordinary sense.

3. Consistency and Independence of the Postulates. We consider the three postulate-sets:

$$\Delta_n\text{: } (A1),\ (A2),\ (M1),\ (M2),\ (D),\ (N_n)\ \ (n > 1).$$

$$\Delta'\text{: } (A1),\ (A2),\ (M1),\ (M2),\ (D),\ (N').$$

$$\Delta''\text{: } (A1),\ (A2),\ (M1),\ (M2),\ (D),\ (N'').$$

As the first five postulates alone are in each case necessary and sufficient for the field properties, we need only ask whether the adjunction of the last postulate permits the existence of a field. E. H. Moore has shown* that every finite field is abstractly equivalent to a Galois field; since the number of elements of a Galois field is always a power of a prime and for every power of a prime one and only one Galois field exists, *the set* Δ_n *is consistent when and only when* n *is a power of a prime*; *it is then categorical.*

Examples of fields of countably and continuously infinite numbers of elements are furnished by the classes of all rational numbers and all real numbers respectively, with

$$a \oplus b = a + b, \qquad a \otimes b = ab.$$

Hence *each of the sets* Δ', Δ'' *is consistent.*†

The consistency of each Δ-set carries with it the independence of the N-postulate in each of the other Δ-sets. The independence of each remaining postulate is shown, simultaneously for the three Δ-sets, in the usual way by the exhibition of systems satisfying all the postulates except the one considered. Agreeing throughout to take for K in Δ_n the n distinct integers modulo n, in Δ' all rational numbers, and in Δ'' all real numbers, we list the independence-systems as follows:

$$[A1]\quad a \oplus b = b; \qquad a \otimes b = a + b.$$

$$[A2]\quad a \oplus b = a; \qquad a \otimes b = a + b.$$

$$[M1]\quad a \oplus b = a + b; \qquad a \otimes b = b.$$

$$[M2]\quad a \oplus b = a + b; \qquad a \otimes b = 0.$$

$$[D]\quad a \oplus b = a + b; \qquad a \otimes b = a + b.$$

Thus *the postulates of each set* Δ_n, Δ', Δ'' *are independent.*

4. Further Considerations on Independence. It will be observed that for each of the independence-systems just given the values of $a \oplus b$ and $a \otimes b$ are defined without exception as elements of K; thus *none of the postulates is deducible from the others even with the aid of the two new postulates*:

($A3$) *If* a *and* b *belong to* K, *then* $a \oplus b$ *belongs to* K.

($M3$) *If* a *and* b *belong to* K, *then* $a \otimes b$ *belongs to* K.

Peculiar interest attaches to the independence-systems for those postulates—($A1$) and ($M1$)—which demand for addition and multiplication our combination-substitute for the associative and commutative laws.

---

* Mathematical Papers Read at the International Mathematical Congress, Chicago (1893), p. 208.

† Neither is categorical. Possible distinct forms of countably infinite fields are discussed by de Séguier, Théorie des groupes finis (1904), p. 51.

Since [$A1$] preserves the associative law for addition and [$M1$] that for multiplication, ($A1$) *is not deducible from the other postulates even with the aid of* ($A3$), ($M3$), *and the associative law for addition*; ($M1$) *is not deducible from the other postulates even with the aid of* ($A3$), ($M3$), *and the associative law for multiplication.*

We are naturally led to ask whether ($A1$) is a consequence of the other postulates together with ($A3$), ($M3$), and the commutative law for addition; and similarly for ($M1$). For the sets Δ', Δ'' the first question is at once answered in the negative. Taking for K all rational numbers or all real numbers, we have the independence-systems:

[$A1$] $$a \oplus b = -a - b; \qquad a \otimes b = ab.$$

We can also construct an independence-system for Δ_n. When n is odd, take for K the n distinct integers modulo n, and define:

[$A1$] $$a \oplus b = \frac{n+1}{2}(a+b); \qquad a \otimes b = a + b.$$

When n is even and greater than 4, take for K the $(n-1)$ distinct integers modulo $(n-1)$, and a special element z; define:

[$A1$] $$a \oplus b = \frac{n}{2}(a+b)$$

unless $a = z$, $b = z$, or $a = b$; $a \oplus z = z \oplus a = a$; $a \oplus a = z$;

$$a \otimes b = a + b$$

unless $a = z$ or $b = z$; $a \otimes z = z \otimes a = z$.

In case $n = 4$, we use the four elements 0, 1, 2, z, with the laws of combination:

[$A1$]

$\oplus$	0	1	2	z
0	z	0	2	1
1	0	z	1	2
2	2	1	z	0
z	1	2	0	z

$\otimes$	0	1	2	z
0	0	1	2	z
1	1	2	0	z
2	2	0	1	z
z	z	z	z	z

For $n = 2$, the associative law is easily deduced from the other postulates. Therefore ($A1$) *is not deducible from the other postulates of* Δ', Δ'', *or of* Δ_n *if* $n > 2$, *even with the aid of* ($A3$), ($M3$), *and the commutative law for addition.*

Let us now study the corresponding question for ($M1$). With the set Δ', choose for K all ordinary complex numbers with rational components; with Δ'', all complex numbers*; we have the independence-definitions:

[$M1$] $$a \oplus b = a + b; \qquad a \otimes b = \bar{a}\bar{b}.$$

---

* As usual, we denote by $\bar{a}$ the conjugate complex number to a.

The results for Δ_n are less simple. Let us assume for a class K all the postulates of Δ_n except ($M1$), and also ($A3$), ($M3$), and the commutative law for multiplication. By Theorem I, K is an abelian group with respect to $\oplus$. We agree to write

$$a \oplus a \oplus \cdots \oplus a \; (\nu \text{ terms}) = \nu a,$$

ν being any positive integer; we have the identities:

$$\nu(a \oplus b) = \nu a \oplus \nu b,$$

and (by continued application of (D))

$$\nu(a \otimes b) = \nu a \otimes b.$$

For any element $a \neq 0$ there are positive integers π such that

$$(\pi + 1)a = a;$$

the least such positive integer π_0 is the period of a, and any other such positive integer π is a multiple of π_0. Let π_0, κ_0 be the periods of the elements a, b respectively. By ($M2$) choose x, y so that

$$a \otimes x = b, \qquad b \otimes y = a.$$

Then

$$(\pi_0 + 1)b = (\pi_0 + 1)(a \otimes x) = (\pi_0 + 1)a \otimes x = a \otimes x = b,$$

$$(\kappa_0 + 1)a = (\kappa_0 + 1)(b \otimes y) = (\kappa_0 + 1)b \otimes y = b \otimes y = a;$$

thus π_0 is a multiple of κ_0 and κ_0 a multiple of π_0, so that $\pi_0 = \kappa_0$. Hence all elements $\neq 0$ have the same period, and by a well-known theorem of group-theory K is an abelian group, with respect to $\oplus$, of order p^μ and type $(1, 1, \cdots, 1)$.

If we choose μ independent generators $u_1, u_2, \cdots, u_\mu$ of the group, any element of K is expressible in the form $\nu_1 u_1 \oplus \nu_2 u_2 \oplus \cdots \oplus \nu_\mu u_\mu$, where the coefficients $\nu_1, \nu_2, \cdots \nu_\mu$ are integers modulo p; we have to deal with a finite linear commutative algebra, in which division by a non zero element is uniquely possible.* In case $\mu = 1$, every element is of the form νu; furthermore

$$\nu u \otimes \nu' u = \nu(u \otimes \nu' u) = \nu(\nu' u \otimes u) = \nu\nu'(u \otimes u);$$

thus the associative law is satisfied, since

$$\nu u \otimes (\nu' u \otimes \nu'' u) = \nu\nu'\nu''[u \otimes (u \otimes u)] = \nu\nu'\nu''[(u \otimes u) \otimes u]$$
$$= (\nu u \otimes \nu' u) \otimes \nu'' u.$$

---

* *Possible*, on account of ($M2$); *uniquely* so, since the form $a \otimes x$ represents an element of K, by ($M3$), and must run through all elements of K as x runs through all elements of K, by ($M2$).

We show finally that if $\mu > 1$, it is possible to find a system in which the associative law fails. To this end take for K the Galois field $GF[p^\mu]$; define:

$$[M1] \qquad a \oplus b = a + b; \qquad a \otimes b = a^p b^p$$

All the laws of addition evidently hold, likewise ($M3$) and the commutative law for multiplication. (D) is also satisfied in view of the identity in the field:

$$(a + b)^p = a^p + b^p.$$

Lastly, ($M2$) is satisfied by choosing

$$x = a^{-1} b^{p^{\mu - 1}}.$$

The associative law fails unless a, b, or $c = 0$, or $a^{p-1} = c^{p-1}$,—surely, then, if $a = b = 1$, $c =$ a primitive root in the field.*

We collect these results as follows: ($M1$) *is not deducible from the other postulates of* Δ', Δ'', *or of* Δ_n *if* n *is a power higher than the first of a prime, even with the aid of* ($A3$), ($M3$), *and the commutative law for multiplication*; ($M1$) *is deducible from these postulates if* n *is a prime*; *if* n *is not a power of a prime, the postulates of* Δ_n *without* ($M1$), *but with* ($A3$), ($M3$), *and the commutative law for multiplication, are inconsistent.*

CORNELL UNIVERSITY,
February, 1913.

---

* In the finite algebras thus defined there is no idemfacient element; hence these algebras are not of the type studied by Dickson, Transactions of the American Mathematical Society, vol. 7 (1906), p. 370 and p. 514.